

(19)

JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **08185361 A**

(43) Date of publication of application: **16.07.96**

(51) Int. Cl.

G06F 12/14
G06F 9/06
G06F 15/78
G11C 16/06

(21) Application number: **06326591**

(71) Applicant: **HITACHI LTD**

(22) Date of filing: **28.12.94**

(72) Inventor: **ITO AKIRA**

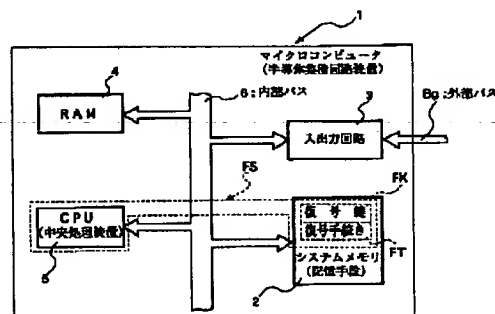
**(54) SEMICONDUCTOR INTEGRATED CIRCUIT
DEVICE**

(57) Abstract:

PURPOSE: To make it difficult to analyze a program by inputting a ciphered program from the external and deciphering the program in a semiconductor integrated circuit device.

CONSTITUTION: A decipher key FK based upon prescribed deciphering algorithm for deciphering a ciphered control program and a deciphering procedure FT for processing the deciphering algorithm by the use of the key FK are stored in a system memory 2 for storing a control program. A CPU 5 temporarily stores a ciphered control program from an external memory or a hard disk in a RAM 4 through an I/O circuit 3, deciphers the program based upon the key FK and the software of the procedure FT, stores the deciphered control program in the memory 2, and erases the contents of the RAM 4. Except a supervisor, the control program inhibits the read of data stored in the memory 2.

COPYRIGHT: (C)1996,JPO



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平 8 - 1 8 5 3 6 1

(43) 公開日 平成 8 年 (1 9 9 6) 7 月 1 6 日

(51) Int. Cl. °	識別記号	序内整理番号	F I	技術表示箇所
G06F 12/14	320	B		
9/06	550	A		
15/78	510	G		
G11C 16/06				

G11C 17/00 520 Z

審査請求 未請求 請求項の数 4 O L (全 7 頁)

(21) 出願番号 特願平 6 - 3 2 6 5 9 1

(22) 出願日 平成 6 年 (1 9 9 4) 1 2 月 2 8 日

(71) 出願人 0 0 0 0 5 1 0 8

株式会社日立製作所

東京都千代田区神田駿河台四丁目 6 番地

(72) 発明者 伊藤 明

東京都青梅市今井 2 3 2 6 番地 株式会社

日立製作所デバイス開発センタ内

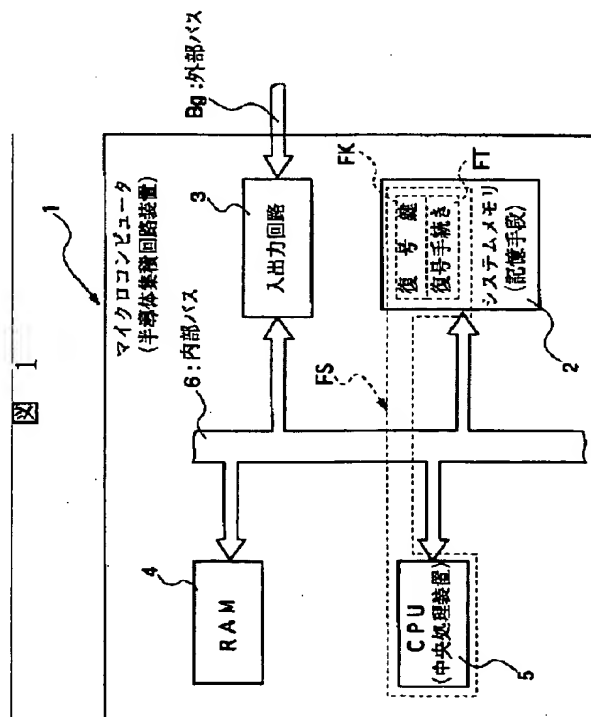
(74) 代理人 弁理士 筒井 大和

(54) 【発明の名称】 半導体集積回路装置

(57) 【要約】

【目的】 暗号化したプログラムを外部から入力し、半導体集積回路装置の内部で復号化を行い、プログラムの解析を困難にする。

【構成】 制御プログラムが格納されるシステムメモリ 2 には、暗号化された制御プログラムを復号化する所定の復号アルゴリズムに基づく復号鍵 F K および復号鍵 F K を用いて復号アルゴリズムを処理する復号手続き F T が格納されている。CPU 5 は暗号化された制御プログラムを外部メモリやハードディスクなどから入出力回路 3 を介して RAM 4 に一旦格納し、復号鍵 F K、復号手続き F T のソフトウェアに基づいて復号化を行い、復号化された制御プログラムをシステムメモリ 2 に格納し、RAM 4 の内容を消去する。制御プログラムはスーパーバイザ以外においてシステムメモリ 2 に格納されているデータを読み出しを禁止する。



【特許請求の範囲】

【請求項 1】 暗号化されたデータを復号化する復号化手段を設け、前記復号化手段により外部バスから入力される暗号化されたデータを復号化することを特徴とする半導体集積回路装置。

【請求項 2】 前記復号化手段が、所定の復号アルゴリズムに基づく復号鍵と前記復号アルゴリズムを処理する復号手続きが格納された記憶手段と、復号化処理を制御する中央処理装置とよりなり、前記外部バスから入力される暗号化されたデータを前記中央処理装置が前記復号鍵および前記復号手続きに基づいて復号化を行うことを特徴とする請求項 1 記載の半導体集積回路装置。

【請求項 3】 前記復号化手段が、所定の前記復号アルゴリズムに基づく前記復号鍵が格納された記憶手段と、前記復号アルゴリズムを処理する復号処理装置とよりなり、前記外部バスから入力される暗号化されたデータを前記復号処理装置が前記記憶手段に格納された前記復号鍵を用いて復号化を行うことを特徴とする請求項 1 記載の半導体集積回路装置。

【請求項 4】 前記記憶手段が、スーパーバイザ以外におけるアクセスが禁止される制御プログラムが格納されるシステムメモリであり、前記データが該半導体集積回路装置の制御プログラムであることを特徴とする請求項 1、2 または 3 記載の半導体集積回路装置。

【発明の詳細な説明】

【 0 0 0 1 】

【産業上の利用分野】 本発明は、半導体集積回路装置に関し、特に、マイクロプロセッサにおける制御プログラムの秘匿に適用して有効な技術に関するものである。

【 0 0 0 2 】

【従来の技術】 本発明者が検討したところによれば、命令格納用メモリである ROM などを内蔵していない半導体集積回路装置では、アドレスバス、データバスおよび制御信号用バスを外部に開放し、これらの信号を用いて外部メモリから命令をロードしている。

【 0 0 0 3 】 なお、ROM などを内蔵していない半導体集積回路装置の外部メモリによる拡張技術について詳しく述べてある例としては、オーム社、1988 年 12 月 20 日発行、湯田幸八、伊藤彰（著）「マイクロコンピュータ入門テキスト」、P 190 がある。

【 0 0 0 4 】 また、本発明者の検討によれば、プログラムを格納するシステムメモリを内蔵している半導体集積回路装置であっても、メモリの大容量化に対応するためにアドレスバス、データバスおよびコントロール信号を外部に開放する外部拡張モードを有しているものがある。

【 0 0 0 5 】 なお、半導体集積回路装置の外部拡張モードについて詳しく述べてある例としては、電波新聞社、昭和 54 年 9 月 1 日発行「マイコン」1979 年 9 月号、P 36 ~ P 37 がある。

【 0 0 0 6 】

【発明が解決しようとする課題】 ところが、上記のような半導体集積回路装置では、次のような問題点があることが本発明者により見出された。

【 0 0 0 7 】 すなわち、外部メモリに命令を格納するためにアドレスバス、データバスおよびコントロール信号が外部開放されているので、信号解析を行うだけで容易に実行命令、またはプログラムが解析されてしまう。

【 0 0 0 8 】 また、外部メモリが ROM であると、プログラムの更新時に着脱を容易にするために IC ソケット上に ROM が実装されている場合があり、この ROM を取り外し、ROM ライタなどによってプログラム解析を行うことも可能である。

【 0 0 0 9 】 さらに、制御プログラムを格納するためのメモリであるシステムメモリが半導体集積回路装置内部に設けられている場合であっても、システムメモリに格納されたプログラムはアクセス保護されていず、ユーザメモリ空間へ容易に読み出されてしまう。

【 0 0 1 0 】 本発明の目的は、暗号化したプログラムを外部から入力し、半導体集積回路装置内部で復号化を行うことによって、容易にプログラムを解析できないようにする半導体集積回路装置を提供することにある。

【 0 0 1 1 】 本発明の前記ならびにその他の目的と新規な特徴は、本明細書の記述および添付図面から明らかになるであろう。

【 0 0 1 2 】

【課題を解決するための手段】 本願において開示される発明のうち、代表的なものの概要を簡単に説明すれば、以下のとおりである。

【 0 0 1 3 】 すなわち、本発明の半導体集積回路装置は、暗号化されたデータを復号化する復号化手段を設け、復号化手段により外部バスから入力される暗号化されたデータを復号化するものである。

【 0 0 1 4 】 本発明の半導体集積回路装置は、前記復号化手段が、所定の復号アルゴリズムに基づく復号鍵と復号アルゴリズムを処理する復号手続きが格納された記憶手段と、復号化処理を制御する中央処理装置とよりなり、外部バスから入力される暗号化されたデータを中央処理装置が復号鍵および復号手続きに基づいて復号化を行うものである。

【 0 0 1 5 】 本発明の半導体集積回路装置は、前記復号化手段が、所定の復号アルゴリズムに基づく復号鍵が格納された記憶手段と、復号アルゴリズムを処理する復号処理装置とよりなり、外部バスから入力される暗号化されたデータを復号処理装置が記憶手段に格納された復号鍵を用いて復号化を行うものである。

【 0 0 1 6 】 本発明の半導体集積回路装置は、前記記憶手段が、スーパーバイザ以外におけるアクセスが禁止される制御プログラムが格納されるシステムメモリであり、前記データが本半導体集積回路装置の制御プログラ

ムであるものである。

【 0 0 1 7 】

【作用】上記した本発明の半導体集積回路装置によれば、暗号化されたデータを復号化する復号化手段を設けることにより、外部バスから入力される暗号化されたデータを半導体集積回路装置の内部で復号化することができる。

【 0 0 1 8 】上記した本発明の半導体集積回路装置によれば、復号処理を専用の復号処理装置ではない中央処理装置で実行することにより復号処理装置を削減でき、復号手続きを変更可能とすることにより融通性を高めることができる。

【 0 0 1 9 】上記した本発明の半導体集積回路装置によれば、専用の復号処理装置で復号化を行うことにより復号化を高速化することができる。

【 0 0 2 0 】上記した本発明の半導体集積回路装置によれば、スーパーバイザ以外におけるアクセスを禁止したシステムメモリの一部に復号鍵および復号手続きを格納することによって、復号処理を秘匿化することができる。

【 0 0 2 1 】それにより、暗号化されたデータ以外の信号の観測を防止でき、制御プログラムの解析、いわゆる、リバースエンジニアリングを困難にすることができる。

【 0 0 2 2 】

【実施例】以下、本発明の実施例を図面に基づいて詳細に説明する。

【 0 0 2 3 】（実施例 1）図 1 は、本発明の実施例 1 によるデータの復号化が行われるマイクロコンピュータの要部ブロック図である。

【 0 0 2 4 】本実施例 1 において、マイクロコンピュータ（半導体集積回路装置）1 には、オペレーティングシステムのカーネルなどの制御プログラムが格納される書き換え可能な不揮発性のメモリであるシステムメモリ（記憶手段）2 が設けられている。

【 0 0 2 5 】このシステムメモリ 2 には、暗号化された制御プログラムなどのデータを復号化する所定の復号アルゴリズムに基づく復号鍵 F K および復号鍵 F K を用いて復号アルゴリズムを処理するプログラムからなる復号手続き F T が格納されており、これら復号鍵 F K および復号手続き F T は、システムメモリ 2 に格納されるので、ユーザは書き換えを任意に行うことができる。

【 0 0 2 6 】暗号化の方式には、暗号化および復号化を同一の鍵で行う対称暗号系方式および暗号化の鍵と復号化の鍵が異なる非対称暗号系方式があり、どちらの方式を用いてもよい。

【 0 0 2 7 】暗号化ならびに復号化は、所定のビット列における交換または反転などの可逆的操作を鍵を用いて制御するものである。

【 0 0 2 8 】マイクロコンピュータ 1 は、外部バス B g

を介してデータの入出力を行う入出力回路 3 および入出力回路 3 から入力された所定のデータを格納する R A M 4 が設けられている。

【 0 0 2 9 】また、マイクロコンピュータ 1 には、マイクロコンピュータ 1 のすべての制御を司る C P U （中央処理装置）5 が設けられ、C P U 5 と復号鍵 F K と復号手続き F T とで復号化手段 F S が構成される。これらシステムメモリ 2、入出力回路 3、R A M 4 および C P U 5 は、内部バス 6 を介して接続されている。

【 0 0 3 0 】さらに、マイクロコンピュータ 1 は、図示しない例外処理回路、M M U （メモリ管理ユニット）、タイマ、S C I および D M A コントローラなどの周辺機能回路が設けられている場合もある。

【 0 0 3 1 】次に、本実施例の作用について説明する。

【 0 0 3 2 】まず、システムメモリ 2 に格納されている制御プログラムを更新する場合を考える。

【 0 0 3 3 】通常、マイクロコンピュータ 1 は、電源が投入されるとシステムメモリ 2 に格納されている制御プログラムを実行するが、起動時のオプション、パーソナルコンピュータ（図示せず）などのキーボードにおける特定組合せのキーを押すまたはマイクロコンピュータ 1 の起動後の制御プログラムにおけるシステム更新メニューを実行することによって、制御プログラムを更新するシステム更新モードとなる。

【 0 0 3 4 】システム更新モードとなったマイクロコンピュータ 1 には、暗号化された制御プログラムが、外部バス B g に接続された外部メモリやハードディスクなどから入出力回路 3 を介して入力され、R A M 4 に一旦格納される。

【 0 0 3 5 】次に、R A M 4 に格納された制御プログラムは、C P U 5 がシステムメモリ 2 に格納されている復号鍵 F K および復号手続き F T のソフトウェアに基づいて復号化を行い、エラーがなければ復号化された制御プログラムがシステムメモリ 2 に格納され、制御プログラムの更新が行われる。また、エラーが発生した場合は、パーソナルコンピュータのモニタなどにエラー表示される。いずれの場合も R A M 4 の復号化された制御プログラムは消去される。

【 0 0 3 6 】さらに、システムメモリ 2 に格納された復号鍵 F K および復号手続き F T は、制御プログラムと同様に、ユーザが任意に書き換えることが可能であるが、スーパーバイザ以外においてシステムメモリ 2 に格納されているデータを読み出すことは禁止されている。

【 0 0 3 7 】本発明では、動作中は常にスーパーバイザの管理下におかれ、ユーザの不当な命令はスーパーバイザが阻止する。

【 0 0 3 8 】また、M M U を用いてシステムメモリはシステムアドレス空間に配置され、ユーザアドレス空間からは見えない。システムコールを発行すると一時的にスーパーバイザモードに移行するが、システムメモリの内容

をユーザアドレス空間にコピーするような処理のシステムコールは実装しないので実行できない。

【 0 0 3 9 】それにより、本実施例 1 においては、制御プログラムを更新する場合に、暗号化された制御プログラムがマイクロコンピュータ 1 に入力され、その制御プログラムをマイクロコンピュータ 1 の内部において復号化してシステムメモリ 2 に格納することによって、制御プログラムなどソフトウェアのプログラム解析を困難にできる。

【 0 0 4 0 】また、スーパーバイザ以外において、システムメモリ 2 に格納されているデータの読み出しが制御プログラムにより禁止されるので、スーパーバイザ以外におけるシステムメモリの読み出しを防止できる。

【 0 0 4 1 】（実施例 2）図 2 は、本発明の実施例 2 によるデータの復号化が行われるマイクロコンピュータの要部ブロック図である。

【 0 0 4 2 】本実施例 2 においては、マイクロコンピュータ 1 に暗号化されたデータである制御プログラムを復号化するアルゴリズム処理部である復号器（復号処理装置） 7 が設けられている。

【 0 0 4 3 】システムメモリ 2 には、復号鍵 F K が格納されている。これら復号鍵 F K および復号器 7 により暗号化されたデータを復号化する復号化手段 F S が構成されている。本実施例においても、復号鍵 F K は、システムメモリ 2 に格納されているので任意に復号鍵 F K の内容を書き換えることが可能である。

【 0 0 4 4 】前記実施例 1 と同様に、入出力回路 3 を介して入力された暗号化された制御プログラムは R A M 4 に一旦格納され、復号器 7 がシステムメモリ 2 に格納された復号鍵 F K を用いて制御プログラムの復号化を行う。

【 0 0 4 5 】次に、C P U 5 が復号の結果コードを判定し、エラーがない場合 R A M 4 において復号化された制御プログラムをシステムメモリ 2 に格納し、エラーが発生した場合はパーソナルコンピュータのモニタなどにエラー表示される。いずれの場合も R A M 4 において復号化された制御プログラムを消去する。

【 0 0 4 6 】さらに、システムメモリ 2 に格納された復号鍵 F K は、制御プログラムと同様に、ユーザが任意に書き換えることが可能となるが、このシステムメモリ 2 には、本実施例 2 においても、スーパーバイザ以外においてシステムメモリ 2 に格納されているデータを読み出すことを禁止している。

【 0 0 4 7 】それにより、本実施例 2 でも、暗号化された制御プログラムがマイクロコンピュータ 1 に入力され、その制御プログラムをマイクロコンピュータ 1 の内部において復号化してシステムメモリ 2 に格納することによって、制御プログラムなどのソフトウェアの解析を困難にでき、スーパーバイザ以外におけるシステムメモリ 2 のデータの読み出しが制御プログラムにより禁止さ

れるので、スーパーバイザ以外におけるシステムメモリの読み出しを防止できる。

【 0 0 4 8 】また、制御プログラムの復号化を専用に行う復号器 7 を設けたことによって、復号化に必要な時間を大幅に短縮することができる。

【 0 0 4 9 】以上、本発明者によってなされた発明を実施例に基づき具体的に説明したが、本発明は前記実施例に限定されるものではなく、その要旨を逸脱しない範囲で種々変更可能であることはいうまでもない。

【 0 0 5 0 】たとえば、前記実施例 1 では、復号鍵 F K および復号手続き F T は、制御プログラムが格納されるシステムメモリ 2 の一部に格納したが、図 3 に示すように、復号鍵 F K および復号手続き F T を格納する専用の R O M （記憶手段） 8 を設け、C P U 5 および R A M （記憶手段） 8 a によって復号化手段 F S を構成してもよい。

【 0 0 5 1 】また、前記実施例 2 でも、復号鍵 F K をシステムメモリ 2 の一部に格納したが、図 4 に示すように、復号鍵 F K を格納する専用の R O M 8 a を設け、復号器 7 および R O M 8 a によって復号化手段 F S を構成してもよい。

【 0 0 5 2 】さらに、システムメモリ 2 が制御プログラムに比べて容量が小さい場合には、図示しない外部メモリに暗号化した制御プログラムを格納し、必要なページまたはセグメント単位に外部メモリから入出力回路 3 を介してスワップインして復号化することも可能である。

【 0 0 5 3 】この場合には、前記実施例 2 の様に、ハードウェアにより構成された復号器 7 を用いれば復号を高速化でき、復号器 7 を並列動作させればさらに高速化することができる。

【 0 0 5 4 】

【発明の効果】本願によって開示される発明のうち、代表的なものによって得られる効果を簡単に説明すれば、以下のとおりである。

【 0 0 5 5 】（ 1 ）本発明によれば、復号化手段により暗号化されたデータを復号化することによって、外部バスから入力される暗号化されたデータを内部で秘密に復号化することができ、データの解析を困難にできる。

【 0 0 5 6 】（ 2 ）さらに、本発明においては、記憶手段に格納された復号鍵と復号手続きに基づいて、中央処理装置が外部バスから入力される暗号化されたデータを復号化することによって、簡単な回路構成で暗号化されたデータを復号化することができる。

【 0 0 5 7 】（ 3 ）また、本発明では、記憶手段に格納された復号鍵を用いて、復号アルゴリズムを処理する復号処理装置を設けることによって、暗号化されたデータの復号化の高速化ができる。

【 0 0 5 8 】（ 4 ）また、本発明によれば、スーパーバイザ以外におけるアクセスを禁止したシステムメモリの一部に復号鍵および復号手続きを格納することにより、

7

復号鍵または復号手続きをユーザが任意に書き換えられ、より簡単な回路構成で外部バスから入力される暗号化されたデータを復号化でき、スーパーバイザ以外のシステムメモリの読み出しを防止できる。

【0059】(5)さらに、本発明においては、上記(1)～(4)により、プログラムがシステムメモリに格納されたパーソナルコンピュータやワークステーションなどのリバースエンジニアリングを困難にでき、暗号化を用いることによって、プログラムなどの配布を公衆回線を用いて行うことも可能となる。

【0060】(6)また、本発明では、非対称暗号系方式を用い、各半導体集積回路装置毎に相異なる復号鍵を設定すれば各半導体集積回路装置は対応する暗号化鍵で暗号化されたデータ以外を正常に復号化できないことから、プログラムの不正コピー防止にも利用できる。

【図面の簡単な説明】

【図1】本発明の実施例1によるデータの復号化が行われるマイクロコンピュータの要部ブロック図である。

【図2】本発明の実施例2によるデータの復号化が行われるマイクロコンピュータの要部ブロック図である。

8

【図3】本発明の他の実施例によるデータの復号化が行われるマイクロコンピュータの要部ブロック図である。

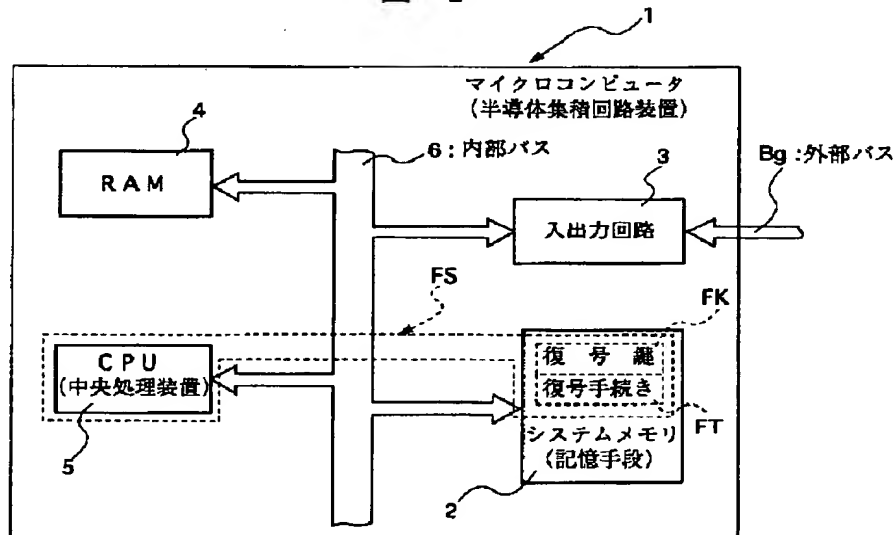
【図4】本発明のさらに他の実施例によるデータの復号化が行われるマイクロコンピュータの要部ブロック図である。

【符号の説明】

- 1 マイクロコンピュータ (半導体集積回路装置)
- 2 システムメモリ (記憶手段)
- 3 入出力回路
- 4 RAM
- 5 CPU (中央処理装置)
- 6 内部バス
- 7 復号器 (復号処理装置)
- 8 ROM (記憶手段)
- 8 a ROM (記憶手段)
- FS 復号化手段
- FK 復号鍵
- FT 復号手続き
- Bg 外部バス

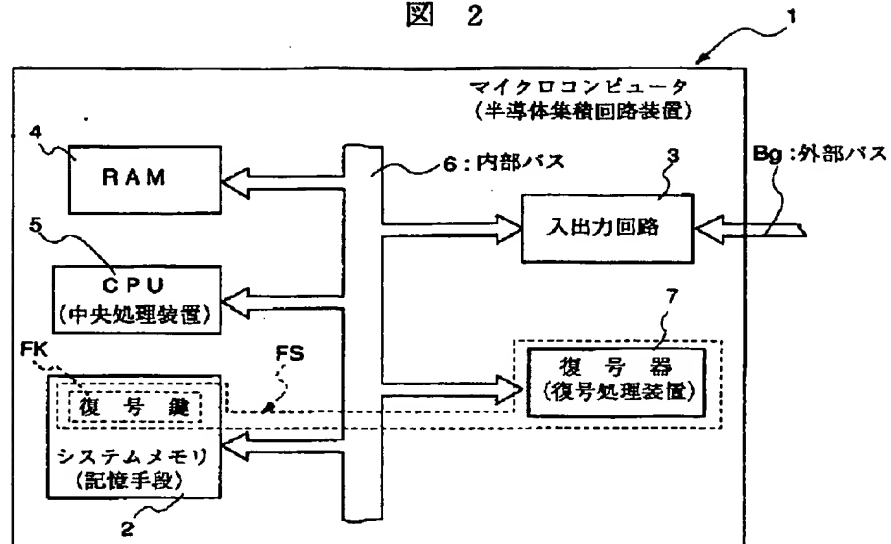
【図1】

図 1



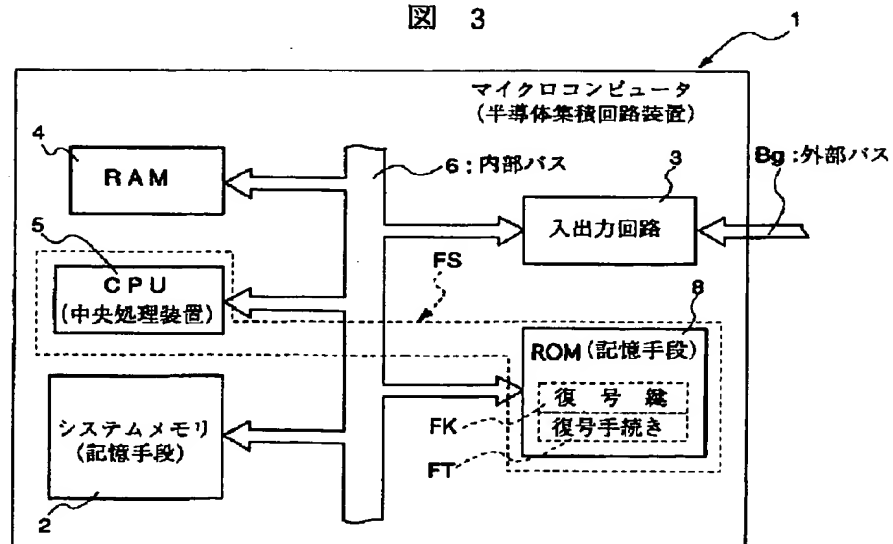
【図 2】

図 2



【図 3】

図 3



【 図 4 】

図 4

